Oxford Global Society

www.oxgs.org

European policies towards Chinese tech companies:

European interests, risk analysis and policy recommendations

Jufang Wang Denis Galligan

December 2021

Published in December 2021 by Oxford Global Society.

About the authors:

Dr Jufang Wang is deputy director of Oxford Global Society and the coordinator of its Digital Technologies cluster. Email: jufang.wang@oxgs.org

Professor Denis Galligan is director of Oxford Global Society and Emeritus Professor in Socio-Legal Studies, Oxford University. Email: denis.galligan@csls.ox.ac.uk

Disclaimer:

Views expressed in this policy report reflect the opinions of individual author (s) and not those of Oxford Global Society.

About Oxford Global Society

We are an independent, non-political think tank based in the UK. In an increasingly politicized and polarized world, we aim to transcend values, ideologies, and national boundaries.

We conduct independent and evidence-based research on selected issues of global interest and importance. Our researchers also provide consultancy for industries, governments and international institutions.

Table of Contents

Executive Summary

1. Despite being initially divided about how to deal with Chinese tech companies (as illustrated in the treatment of Huawei), Europe has now adopted a more coordinated approach and aligned closer with the United States. Currently, most European countries have adopted a policy of restricting or excluding Chinese telecoms firms from the rollout of 5G networks and imposed stricter scrutiny over Chinese investment in Europe's tech sector.

2. While Europe shares common democratic values with the U.S., it has its own digital values and interests. For Europe, achieving digital sovereignty and global technological leadership are its core interests in the digital age. Achieving digital sovereignty means reducing digital dependence on non-European countries (especially the U.S.), data control, and building a strong digital industry. Global technology leadership requires Europe to set global technology standards and promote its own digital values.

3. There are three types of perceived risks—geopolitical, security and economic—associated with Chinese tech companies in Europe. Our analysis concludes that some of the perceived risks are real and reasonable, and others are not evidence-based and mostly geopolitics-driven.

4. Based on the digital interests of Europe and our analysis of the perceived risks linked to Chinese tech companies, we make the following policy recommendations for European countries:

- Prioritising technical solutions over a geopolitical approach in mitigating risks that are inherent in emerging technologies or associated with Chinese companies;

- Strengthening Europe's regulatory power to protect and enhance its digital sovereignty, to tackle potential risks, and to establish global technology leadership;

- Making Europe a global high-tech hub by attracting global talents, investment and companies and cultivating local tech giants through "light protectionism";

- Supporting a multilateral approach in setting global technical standards for critical and emerging technologies and shaping the development of global standards by mediating between the US and China;

- Promoting European digital values through cooperation and engagement with other parties.

1 Introduction

Digital technologies are increasingly at the center of competition between countries. Since taking office in January this year, American President Joe Biden has continued the path started by his predecessor in targeting Chinese technology companies by blacklisting many more of them and imposing on them sanctions and export control.[1] At the same time, the U.S. has been pressuring allies to join its action. Against this background, the choice of Europe is crucial in shaping the future direction of global technology competition.

Initially, Europe was divided on how to position itself amid US-China tech rivalry, and many European countries resisted pressure from the Trump administration to exclude Chinese telecommunications giant Huawei from the rollout of their 5G networks.[2] However, the last two years saw many European countries changing course regarding their policies towards Chinese tech companies and aligning closer with the US. This development was epitomised in the inaugural joint statement of the US-EU Trade and Technology Council (TTC) in late September 2021. The statement emphasized that the two sides would strengthen their coordination and cooperation in technology areas including ensuring the security of critical and emerging technologies such as 5G and Artificial Intelligence (AI), investment screening, export control, and global standards development. While China was not mentioned in the statement, observers familiar with US-China tech rivalry would have no difficulty working out which country the US-EU coordination was aimed at.

We now raise a series of questions regarding the policies of European countries towards Chinese tech companies: What are the core interests of Europe regarding global technology competition? How should Europe position itself amid US-China tech rivalry to optimise its own interests? Regarding Europe's assessment of risks posed by Chinese tech companies, are they empirical and evidence-based, or are they mostly from a geopolitical logic? Are there viable ways to mitigate the risks other than excluding Chinese high-tech companies?

This report begins with a brief review of Europe's current policies towards Chinese tech companies. It then identifies and discusses European interests regarding global

[1] Reuters (9 July 2021). *EXCLUSIVE U.S. set to add more Chinese companies to blacklist over Xinjiang.* https://www.reuters.com/world/china/exclusive-us-set-add-more-chinese-companies-blacklist-over-xinjiang-2021-07-09/

[2] The New York Times (17 March 2019). U.S. campaign to ban Huawei overseas stumbles as allies resist. https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html

technology competition, followed by an analysis of the perceived risks associated with Chinese high-tech companies in Europe. Last, we will make a series of policy recommendations for European countries in dealing with Chinese tech companies and in mitigating potential risks. We argue that while concerns towards Chinese tech companies are understandable, it is not in the interest of Europe to follow a geopolitical approach of excluding them from European markets. Instead, to achieve digital sovereignty and become a global tech leader, we conclude that, first, Europe should resort more to **technical solutions** to tackle potential risks; secondly, should rely more on its **regulatory power** to foster innovation and growth of local tech companies; and thirdly, should adopt a more **multilateral approach** to set global standards for emerging technologies and to promote European digital values.

2 European policies towards Chinese tech companies

So far, Europe has adopted a coordinated approach, both within Europe and with the US, towards Chinese tech companies. This approach is most prominent in European countries' policies towards Huawei and other Chinese telecommunications firms in the rollout of 5G networks. Huawei is the global market leader in network equipment, accounting for 30% of mobile base stations worldwide in 2021.[3] It was also the market leader in many European countries. For example, in the UK, Huawei accounted for 44% of the fixed access Full Fibre networks and 35% mobile access networks in 2019.[4] Initially, Europe was divided about the treatment of Huawei. For instance, while various European countries like Poland and Czech Republic signed agreements with the US to exclude Huawei from their markets, the UK, one of America's closest allies, decided to allow Huawei to participate in its non-core 5G networks with a market share capping at 35%.[5]

However, pressure from the US, including threats to cease intelligence sharing, changed the attitudes of many European countries towards Huawei. In July 2020, the UK took a U-turn and decided to phase out the company by 2027.[6] In explaining UK's new policies towards Huawei, Alistair Bunkall, defence and security correspondent of Sky News, observed, "The decision was influenced by heavy lobbying from

[3] Statista. *Mobile base station vendor market share worldwide from 2019 to 2021.* https://www.statista.com/statistics/1134472/global-mobile-base-station-vendor-market-share/

[4] Department for Digital, Culture, Media & Sport (UK). July 2019. *UK telecoms supply chain review report.*

[5] BBC News (28 January 2020). *Huawei set for limited role in UK 5G networks.* https://www.bbc.co.uk/news/technology-51283059

[6] BBC News (14 July 2020). *Huawei 5G kit must be removed from UK by 2027.* https://www.bbc.co.uk/news/technology-53403793

Washington…The UK was threatened: ban Huawei or impact intelligence sharing [with the US]."[7] The EU also took actions to coordinate its member states' response to risks associated with 5G networks. In October 2019, the EU published a coordinated risk assessment of 5G networks, which identified a series of threat scenarios and threat actors targeting 5G networks. The listed threats include local or global network disruption, spying, modifying or rerouting the traffic/data; among the listed various threat actors, the report emphasized that threats "posed by States or State-backed actors, are perceived to be of highest relevance".[8] Following this report, the EU proposed in January 2020 a 5G networks Toolbox, recommending member states to apply "restrictions for suppliers considered to be high risk- including necessary exclusions to effectively mitigate risks- for key assets".[9] These two documents are crucial to the EU's coordinated efforts regarding 5G networks security.

Currently, most EU countries have proposed or passed legislations restricting or excluding "high-risk" suppliers in their 5G networks. In April 2021, Germany passed IT Security Law 2.0, which restricts the role of "untrustworthy" suppliers of 5G technology and gives the government powers to block contracts concerning critical 5G components.[10] The decision of Germany, which had long been wary about alienating China (Germany's biggest trade partner since 2016), suggests that the tide in Europe may have turned against Chinese tech companies. While some EU countries like France and Italy haven't passed laws to ban Huawei, their governments have the power to block relevant deals. For example, French Cybersecurity Agency planned to phase out Huawei by 2028.[11] In other European countries like Portugal and Netherlands, while the governments haven't decided on their policies towards Huawei, major local telecom operators have announced their decisions not to choose Huawei.[12] Such decisions are easy to understand, as European Commissioner Thierry Breton pointed out, "If they [telecom operators] choose a 'high-risk 5G supplier,' the board members may be liable if something happens."[13]

---

[7] Sky News (24 November 2020). *New law unveiled to make UK 5G network safer*. https://news.sky.com/story/new-law-unveiled-to-make-uk-5g-network-safer-12140684

[8] European Union. October 2019. *EU coordinated risk assessment of the cybersecurity of 5G networks*, p.13.

[9] European Union. *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*. p.12.

[10] POLITICO (23 April 2021). *Germany falls in line with EU on Huawei*. https://www.politico.eu/article/germany-europe-huawei-5g-data-privacy-cybersecurity/

[11] Politico (23 July 2020). *France introduces de facto ban on Huawei 5G equipment by 2028.* https://www.politico.eu/article/france-introduces-de-facto-ban-on-huawei-5g-equipment-by-2028/

[12] Euractiv (19 May 2021). *EU countries keep different approaches to Huawei on 5G rollout.* https://www.euractiv.com/section/digital/news/eu-countries-keep-different-approaches-to-huawei-on-5g-rollout/

[13] European Commission (30 September 2020). Meeting between U.S. Under Secretary of State Krach and Commissioner Breton on Secure Telecommunications Infrastructure and Digital agenda.

Apart from 5G networks, Europe has also adopted a tougher policy towards Chinese companies in wider technology areas, among which is the investment of Chinese companies in local tech companies. In April 2021, the UK's National Security and Investment Act became law, which tightens investment screening against "potentially hostile" foreign direct investment (FDI) on the grounds of national security.[14] While this law does not target Chinese companies in particular, it is widely seen as UK's response to "concerns that sensitive technologies could leak to China and other countries".[15] Based on this law, the UK government is currently reviewing the purchase of the UK's largest semiconductor producer Newport Wafer by a Dutch firm that is wholly owned by China's Wingtech.[16] In 2019, the EU adopted a framework for FDI screening (operational requirements for its full application added in 2020), which helps the Union and member states to coordinate their actions on foreign investment. As Bendiek and Lippert (2020) observe, the EU "specifically has China in its sight" in adopting this regulation, because it deems that China is seeking to "buy its way strategically" into EU's high-tech areas, such as AI, robotics and biotechnology.[17] In recent years, many EU member states including France, Germany and Italy updated their FDI screening mechanisms and strengthened their scrutiny over Chinese FDI, resulting in several acquisitions by Chinese firms being blocked.[18]

Meanwhile, Europe has strengthened its coordination with the US in the technology area. During the Trump administration, some European countries including the UK and Poland supported the U.S.-initiated "Clean Network" scheme which explicitly called on "freedom-loving countries" to ban Chinese tech companies.[19] However, it was not until President Biden took office that the transatlantic coordination around

---

https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/meeting-between-us-under-secretary-state-krach-and-commissioner-breton-secure-telecommunications_en

[14] The UK government (29 April 2021). *National security bolstered as bill to protect against malicious investment granted royal assent*. https://www.gov.uk/government/news/national-security-bolstered-as-bill-to-protect-against-malicious-investment-granted-royal-assent

[15] Nikkei Asia (2 May 2021). *UK puts foreign investment under microscope to prevent tech leaks.* https://asia.nikkei.com/Politics/UK-puts-foreign-investment-under-microscope-to-prevent-tech-leaks

[16] The Guardian (7 July 2021). *UK to review purchase of semiconductor producer by Chinese-owned firm.* https://www.theguardian.com/business/2021/jul/07/uk-to-review-purchase-of-semiconductor-producer-by-chinese-owned-firm

[17] Bendiek, A. & Lippert, B. (2020). Positioning the European Union within the Sino-American Rivalry. In: Lippert, B., & Perthes, V. (Eds.). *Strategic rivalry between United States and China: causes, trajectories, and implications for Europe*. pp 49-50. (SWP Research Paper, 4/2020). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit.

[18] MERICS (16 June 2021). *Chinese FDI in Europe: 2020 update*. https://merics.org/en/report/chinese-fdi-europe-2020-update

[19] The U.S. government. *The Clean Network*. https://2017-2021.state.gov/the-clean-network/index.html

technology policies was greatly deepened under the afore-mentioned TTC framework, launched in June during Biden's visit to Brussel. In the inaugural joint statement of the TTC in September, the two sides announced that they "stand together" against unfair trade practices and misuse of technologies like social scoring systems (piloted by China).[20] In addition, both sides mentioned the need for wider efforts with "like-minded partners". These developments manifest that the Biden administration is adopting a cyberspace policy similar to its predecessor—building an alliance of "like-minded" nations to contain countries like China and Russia—only with more success.

It must be noted that although Europe has adopted a more coordinated approach towards Chinese tech companies, there still exist substantial differences among European countries and between Europe and the US. For example, regarding the role of Huawei, while most EU countries follow the instructions given in the EU's 5G Networks risk assessment and the 5G toolbox documents, several different approaches have been adopted within the bloc. An analysis from the Euractive identified three different approaches: (1) The hardliners (some Scandinavian countries like Sweden and Denmark and various Eastern European countries like Poland and Czech Republic); (2) The interventionists (such as France, Italy and Finland whose governments have the power to intervene in deals) ; (3) The bureaucrats and the undecided (such as Spain, Portugal, and the Netherlands, which have taken a more independent approach that mainly relies on bureaucratic procedures rather than political evaluations).[21] In addition, compared to America's aggressive and punitive approach (or "decoupling" approach), European countries' policies towards Chinese tech companies are still much softer and more moderate. Their current policies seem to be largely in response to U.S. pressure, although the lobbying efforts of the U S. did ignite debates in Europe about risks linked to critical infrastructure like 5G networks and emerging technologies. So far, Europe's restrictions on Chinese tech firms are relatively limited, focusing on 5G network suppliers and Chinese investment in key European technology companies (e.g., semiconductor and AI firms).

3 European interests in digital technologies

While sharing democratic values and many security concerns over Chinese tech companies with the US, Europe has its own interests and values in digital areas. We

[20] European Commission. *EU-US Trade and Technology Council Inaugural Joint Statement.* https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951

[21] Euractiv (20 May 2021). *EU countries keep different approaches to Huawei on 5g rollout.* https://www.euractiv.com/section/digital/news/eu-countries-keep-different-approaches-to-huawei-on-5g-rollout/

have identified two main interests of European countries in the digital age: digital sovereignty and global technology leadership. The former refers to Europe's digital autonomy and independence, while the latter means Europe's capacity in setting global standards and promoting European values in a digital world. European countries' policies towards Chinese tech companies relate to both of these interests. It is necessary to note that, although this report focuses on European policies towards Chinese tech companies, European interests in the digital world go much wider than tackling potential risks linked to China. They also concern the dominance of American "big techs" in European markets, data security and the innovative use of data, the position of Europe in the global digital economy, as well as the capacity of Europe to set global technical standards for critical and emerging technologies and to promote its own digital values. In this section, we discuss European interests mainly in reference to the EU, although these interests are largely relevant to other European countries. While there certainly exist competing national interests among European countries, here we focus on the digital interests shared by most countries.

3.1 Digital sovereignty

In recent years, "digital sovereignty" has become a term frequently used by policy makers in the EU, both at the EU-level and member states level. In its strategy document "A Europe fit for the digital age", the European Commission states, the EU is determined to make this decade Europe's "Digital Decade", and Europe must now "strengthen its digital sovereignty and set standards, rather than following those of others".[22] In July 2020, the German government announced, in its official programme for its presidency of the European Council, that it intended to "establish digital sovereignty as a leitmotiv of European digital policy".[23] The meaning of digital sovereignty, a contested concept, is considered below.

The EU's increasing quest for digital sovereignty stems from concerns over the influence of non-EU technology companies in economic, political, security and social areas. As Tambiama Madiega from European Parliamentary Research Service notes, the EU worries that the citizens, businesses and member states of the Union "are gradually losing control over their data, over their capacity for innovation, and over their ability to shape and enforce legislation in the digital environment".[24] The rising

[22] European Union. "A Europe fit for the digital age". https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

[23] European Association for Digital Transition (30 July 2020). *Merkel committed to the EU's digital sovereignty*. https://digitalforeurope.eu/merkel-committed-to-the-eus-digital-sovereignty

[24] Tambiama Madiega (2020). *Digital sovereignty for Europe*. EPRS Ideas Paper. European Parliament.

US-China tensions regarding technologies are "an additional incentive for Europe to develop its own digital capabilities", as it risks "becoming a battleground in their struggle for tech and industrial supremacy".[25] In parallel, the Covid-19 pandemic has demonstrated the critical importance of digital technologies and made "Europe's digital transformation and sovereignty a question of existential importance".[26]

Digital sovereignty, increasingly used by both authoritarian (e.g., China) and democratic countries (e.g., European countries), has different connotations in different contexts.[27] In the case of China, the definition of "digital sovereignty" (or Internet sovereignty) is often vague and broad, as in the words of President Xi Jinping: a state has the right "to choose its online development path, its network management model and its public Internet policies, and to equal participation in international cyberspace governance."[28] As for Europe, we identified three dimensions of digital sovereignty: (1) reducing dependence on non-European countries in digital areas; (2) data control, including data security and data use; (3) building Europe into a global technology hub.

Reducing digital dependence

Dependence on American tech giants has become an increasing concern for Europe in recent years. American tech companies, such as Google, Facebook, Amazon, Apple, Microsoft, Uber, and Airbnb, dominate European markets in almost all digital services including search, social media, e-commerce, cloud, and online travel and accommodation platforms. Europe has wakened to this "neocolonial" dependence on American tech companies, and has taken a series of measures, such as introducing a digital services tax, fining American tech giants for anti-competition practices, and considering new industrial policies to foster local tech giants, in hope of regaining its digital sovereignty.[29]

The increasing presence of Chinese companies, and the consequential dependence on them, emerges as another concern for Europe regarding digital dependence. However, Europe's reliance on American tech giants far exceeds its dependence on Chinese companies. For example, while Chinese telecommunications firms like Huawei and ZTE provided over 40% of Europe's 4G Radio Access Network (RAN)

[25] Carla Hobbs (ed.). (July 2020). Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry. *European Council on Foreign Relations*.
[26] Ibid.
[27] Pohle, Julia & Thiel, Thorsten (2020). Digital sovereignty. *Internet Policy Review*, *9*(4), 1-19.
[28] Rogier Creemers (2020). China's conception of cyber sovereignty. *Governing Cyberspace: Behavior, Power and Diplomacy*, 107-145 (p.109).
[29] Carla Hobbs (ed.). (July 2020). *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry.* European Council on Foreign Relations. P.10

equipment by 2020,[30] they don't have much competitive advantage compared to European companies Nokia and Ericsson. As some European observers note, from a digital sovereignty perspective, the US is "the biggest problem" for Europe, while China, both an economic and political competitor in the digital realm, may be "the biggest fear".[31]

Data control

Data control has at least two dimensions. One dimension is data use. It is estimated that 92% of data generated in the West are stored in the US.[32] This is a major disadvantage for Europe, as data is an essential resource for digital services and technology development (especially in the area of AI). To increase control over data, Europe initiated the Gaia-X project, which aims to reduce reliance on international cloud giants, and encourages European businesses to look to home-grown solutions, protected by European data laws.[33] European countries are also placing more emphasis on data use. For example, the Data Strategy of Germany, published in January 2021, states that the aim of this strategy is to "significantly increase innovative and responsible data provision and data use".[34]

Another dimension is data security. The EU's General Data Protection Regulation (GDPR), which took effect in May 2018, sets out rules to strengthen European citizens' control and rights over their personal data and addresses cross-border data transfer outside the EU and the European Economic Area (EEA). Given that non-European (mostly American) tech companies dominate digital services in European markets, protecting European individuals' personal data from misuses by foreign companies has become an important issue to Europe. In July 2020, the EU Court of Justice invalidated the US-EU Privacy Shield arrangement regarding data transfer on account

[30] Strand Consult. *Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks.* https://strandconsult.dk/understanding-the-market-for-4g-ran-in-europe-share-of-chinese-and-non-chinese-vendors-in-102-mobile-networks/

[31] Carla Hobbs (ed.). (July 2020). Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry. European Council on Foreign Relations. P.10

[32]Oliver Wyman (an American management consulting firm). "European Digital Sovereignty." https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/october/European%20Digital%20Sovereignty.pdf

[33] TechRepublic. What is Gaia-X? A guide to Europe's cloud computing fight-back plan. https://www.techrepublic.com/article/what-is-gaia-x-a-guide-to-europes-cloud-computing-fight-back-plan/

[34] German government (2021). Data Strategy of the Federal German Government. Page 6. https://www.bundesregierung.de/resource/blob/998194/1950610/fb03f669401c3953fef8245c3cc2a5bf/datenstrategie-der-bundesregierung-englisch-download-bpa-data.pdf?download=1

of concerns over "invasive US surveillance programmes".[35] Data security also concerns espionage threats. While espionage threats from China or Chinese tech companies has become a popular narrative in the West (which will be analysed in the next section), the Edward Snowden case in 2013 revealed that the US intelligence agencies had spied on global leaders including many from the EU.[36] This June, a Danish public broadcaster published allegations that Danish intelligence agencies had helped the U.S. National Security Agency to spy on EU leaders.[37]

Building a strong digital industry

The lack of European digital companies with global influence is widely seen as a "key European disadvantage" in achieving its digital sovereignty.[38] To overcome this shortcoming, the EU has set a series of targets for the EU's digital industry. A major objective is to double the number of EU *unicorns* (a "unicorn" is a private company valued at over $ 1 billion) by 2030. By July this year, Europe had produced a total of 289 unicorns, with 37 reached *decacorn* ($ 10 billion valuation) status; in comparison, the US and China have 134 and 36 decacorns respectively.[39] Regarding digital infrastructure, the EU's set goals include ensuring gigabit for everyone and 5G everywhere; to double EU share in global production of cutting-edge semiconductors to 20% by 2030; and to reach 10, 000 climate neutral highly secure edge nodes and to develop the first computer with quantum acceleration.[40]

As for cutting-edge technologies, the EU has identified AI, which has the potential to tackle many challenges and improve the quality of people's lives, as a priority area. The EU and some European countries like Germany have expressed the ambition to become leading AI centres of the world. At the EU level, the European Commission has planned to invest EUR 1 billion per year in AI and aims for over 25% of all industrial

[35] European Parliament. The CJEU judgment in the Schrems II case. https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

[36] The Guardian (25 October 2013). *NSA monitored calls of 35 world leaders after US official handed over contacts* https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

[37] BBC News (31 May 2021). *NSA spying row: Denmark accused of helping US spy on European officials.* https://www.bbc.co.uk/news/world-europe-57302806

[38] Carla Hobbs (ed.). (July 2020). *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*. European Council on Foreign Relations. P.11

[39] Dealroom (22 July 2021). *The rise of European decacorns*. https://dealroom.co/blog/the-rise-of-the-european-decacorn

[40] European commission. *Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030.* https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983

and personal service robots being produced in Europe by 2030.[41] Among member states, almost all European countries have developed their own AI strategies and set aside funding to facilitate its promotion. For instance, German federal government has committed a total of EUR 5 billion by 2025 for the promotion of AI,[42] while the French government has dedicated EUR 1.5 billion to the development of AI by 2022.[43]

3.2 Global technology leadership

In addition to achieving digital sovereignty, Europe aspires to become a global leader in digital technology. This aspiration extends to two areas: setting global technology standards and promoting Europe's digital values. It is worth noting that while some observers consider global technology leadership part of Europe's strategy for digital sovereignty, we treat them as two different core interests, given that we define digital sovereignty in a relatively narrow sense as digital autonomy and independence.

Setting global standards

As mentioned above, Europe strives to "set standards", rather than "following those of others". The setting of technical standards for critical and emerging technologies, such as AI and Internet of Things (IoT), is an arena of fierce competition between companies and national states. The capability of shaping technology standards adds to the geopolitical power of a country or a region like the EU, and it also means economic interest for the relevant patent holders. For Europe, "setting standards" extends to regulatory standards. For example, the GDPR has become the model for many national data protection laws outside the EU, such as Japan, South Korea, Brazil, Argentina, and Kenya (with China being a recent example).[44] The impact of GDPR has demonstrated the regulatory power of Europe in digital areas. Currently, the EU is working on Digital Services Act and Digital Markets Act that deal with the obligations and accountability of intermediaries and fair competition around large platforms (or online "gatekeepers") respectively. These proposed EU-wide regulations are expected to have profound impact on the governance of online intermediaries, including infrastructural platforms around the world.

---

[41] European Commission. *Excellence and trust in artificial intelligence.* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en

[42] European Commission. *Germany AI Strategy Report*. https://knowledge4policy.ec.europa.eu/ai-watch/germany-ai-strategy-report_en

[43] European Commission. *France AI Strategy Report.* https://knowledge4policy.ec.europa.eu/ai-watch/france-ai-strategy-report_en

[44] European Commission (22 May 2019). General Data Protection Regulation: One year on. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610

Promoting European values

Upholding and promoting EU values in the digital age is also part of Europe's core interests. EU has listed a series of digital rights and principles for Europeans, which mainly include freedom of expression, data and privacy protection, a secure online environment, environment-friendly digital systems, human-centred and trustworthy algorithms (i.e., safe, transparent, ethical, unbiased and under human control), and so on.[45] Plainly European countries hold dear to these values. Given that Europe and China have differences in fundamental values and criteria for human rights, it is not surprising that Europe has structural distrust of China's authoritarian governing system and thus in Chinese tech companies.

4 Analysis of perceived risks to Europe

In recent years, many European countries, politicians and lawmakers have echoed American accusations of Chinese tech companies, such as conducting espionage for the Chinese government, stealing Western technologies, and getting involved in China's "mass surveillance" projects. In this section, we aim to conduct an evidence-based analysis of the perceived risks and concerns associated with Chinese tech companies in Europe. We have identified three types of risks or concerns: geopolitical risks, security risks, and economic risks. These risks are often entwined and interconnected. For example, user data not only concern security, but are also crucial economic resources. Likewise, ensuring the safety of 5G networks is an issue of national security, as well as an issue of geopolitical importance and economic growth. What we conclude from our analysis is that some of the perceived risks and concerns linked to Chinese tech companies are real and viable, and others are not evidence-based but mostly geopolitics-driven.

4.1 Geopolitical risks

US-China technology rivalry has caught Europe in the middle. On the one hand, if European countries allow Chinese companies, such as Huawei and ZTE, to participate in their 5G networks rollout, they risk displeasing the US and even retaliation, as well as the risk of damaging the transatlantic alliance. On the other hand, in choosing to align with the US and banning Chinese companies like Huawei, Europe risks

[45] European Commission. Digital citizenship: rights and principles for Europeans. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

damaging its economic cooperation with China, the second biggest trade partner of the EU after the US.[46] Moreover, for the EU, a fragmented policy towards Chinese tech companies would further divide the Union, adding to its geopolitical risks at a time of global technology competition.

While Europe may be unwilling to pick sides between the US and China to avoid damaging its interests, it is unimaginable that it would keep an equidistant position between the US and China. Despite China being a crucial trade partner, Europe has fundamental differences with it over political values and human rights issues. In 2019, the EU identified China as a "systemic rival promoting alternative models of governance".[47] In contrast, Europe shares with the US basic democratic values and governing rules, such as democratically elected governments, an independent judiciary and the rule of law. Equally important is that the EU and the US share a wide range of common interests across political, economic and security areas. For instance, in the security domain, the US has many bilateral and multilateral agreements with European countries (such as through NATO) and shares intelligence with its European allies.

Due to Europe's geopolitical concerns over Chinese companies, it is reasonable that many European countries are concerned about dependence on Chinese telecoms firms like Huawei and ZTE for 5G network equipment. In July 2019, the UK published a review report on its Telecoms supply chain, which concluded that there is "a high risk of increasing dependence on a single vendor [i.e. Huawei]" in the fixed and mobile access network segments.[48] The report also mentioned the following potential risks: "commercial failure or the imposition of certain types of sanctions affecting the ability of a 5G equipment supplier to continue to provide the required level of service".[49] The EU's coordinated risk assessment document highlights similar risks. It notes that "important vulnerabilities" stem from reliance on certain suppliers, and EU-based operators may be exposed to risks caused by a supplier under commercial pressure, due to factors like "being placed under sanctions."[50]

---

[46] European Commission. *Countries and regions: China*. https://ec.europa.eu/trade/policy/countries-and-regions/countries/china/

[47] European commission. *EU-China—a strategic outlook*. https://ec.europa.eu/info/sites/default/files/communication-eu-china-a-strategic-outlook.pdf

[48] Department for Digital, Culture, Media & Sport (UK). July 2019. *UK telecoms supply chain review report*, p.29. https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference

[49] Ibid. p.24.

[50] European Union. October 2019. *EU coordinated risk assessment of the cybersecurity of 5G networks*, p.23.

We consider this risk linked to disrupted equipment supply caused by sanctions on certain suppliers (e.g., Chinese telecoms firms) to be real and viable in the current geopolitical environment. Due to sanctions on Huawei from the US, which include restrictions on the sale of hardware and software to the company, it is not clear whether or when the Chinese company's capacity to provide 5G network equipment will be affected. A breakdown by Nikkei of Huawei's core base station unit for 5G networks revealed that the company still remained heavily dependent on U.S. made chips and components, which accounted for nearly 30% of the product in value terms.[51] This reliance on American products and technologies makes Huawei vulnerable in providing 5G equipment in the future. It is worth noting that although Huawei's mobile phone production has already been severely damaged by American sanctions,[52] there is no evidence that the company's capacity in delivering 5G equipment in China and overseas markets has so far been affected, due to its high stock of relevant chips.

As the West now sees China as a "strategic rival" or "systemic rival", Europe's geopolitical concerns over Chinese tech companies will not go away in the foreseeable future. However, decisions based on geopolitical concerns may have serious consequences for Europe. First, excluding Chinese telecoms firms and removing existing equipment provided by them means that European countries have to pay a substantial price. For example, the UK government estimated that phasing out Huawei would delay the country's 5G networks rollout by two to three years and cost up to £2bn.[53] More importantly, excluding Chinese telecoms firms from Europe (and the West in general) would further disrupt global supply chains and the development of global technology standards for 5G and the future 6G, due to the fact that Chinese firms like Huawei hold many essential patents that are approved and included in the 5G standard by the international standardization body 3GPP.[54] As Swedish telecoms giant Ericsson President and CEO Börje Ekholm warned in an interview, the "geopolitical situation" increases the likelihood of "further industry split, separation of

[51]Nikkei Asia (12 October 2020). Huawei's base station teardown shows dependence on US-made parts. https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-s-base-station-teardown-shows-dependence-on-US-made-parts

[52] Cnet (16 November 2020). *Huawei is selling off Honor phone business to 'ensure its own survival'.* https://www.cnet.com/tech/mobile/huawei-is-selling-off-honor-phone-business-to-ensure-own-survival/

[53] ComputerWeekly (15 July 2020). *UK comms industry counts the cost of Huawei tech ban.* https://www.computerweekly.com/news/252486165/UK-comms-industry-counts-the-cost-of-Huawei-tech-ban

[54] Observatorio Nacional 5G (16 February 2021). *The exclusion of Huawei and ZTE in 5G networks will have severe consequences, warn Ericsson and ABI*. https://on5g.es/en/the-exclusion-of-huawei-and-zte-in-5g-networks-will-have-severe-consequences-warn-ericsson-and-abi/

global value chains and separation of global standards for mobile telecommunications."[55]

Moreover, even if European countries are willing to pay the economic price in exchange for mitigated geopolitical risks, it is possible that phasing out equipment from Chinese companies may also increase risks linked to 5G networks. This is because the current market of 5G networks equipment is very concentrated in only a few major end-to-end global suppliers. As a result, for most European countries, after excluding Chinese firms Huawei and ZTE, there are only two European firms Nokia and Ericsson to choose from. As the afore-mentioned risk assessment of 5G network equipment by the EU and the UK concluded, reliance on any "single" vendor for critical infrastructure would bring important vulnerabilities to the networks.[56]

4.2 Security risks

Security concerns over Chinese tech companies in Europe (and the West generally) mainly centre on espionage, sabotage, and content censorship. All these concerns link to structural distrust of China's governing system and the relationship between the Chinese state and tech firms. Western officials and lawmakers claim that due to the nature of China's authoritarian governing system, Chinese tech companies can be used by the government to collect intelligence or cause disruption to the digital infrastructure overseas. Similarly, Western observers worry that Chinese companies cannot refuse to cooperate with the government if required to disclose personal information of overseas users or conduct content censorship on behalf of Beijing.

Espionage and sabotage risks

Regarding the espionage and sabotage risks linked to Chinese tech companies, several justifications have been suggested in the West: (1) China's National Intelligence Law (2017) obliges Chinese companies to assist intelligence services in collecting intelligence; (2) Chinese companies like Huawei have been accused (or suspected) of installing "backdoors" in their equipment for espionage or sabotage purposes; (3) Chinese companies have exported surveillance technologies to overseas markets including European countries. Our following analysis revolves around these three points.

[55] Verdict (25 May 2021). *Ericsson warns of losing business in China over Sweden's Huawei ban.* https://www.verdict.co.uk/ericsson-china-sweden/

[56] European Union. October 2019. EU coordinated risk assessment of the cybersecurity of 5G networks, p.23.

First, we carefully examined the original texts of China's intelligence law, which states:

> **Article 7**: Any Chinese organizations and citizens should support, assist, and cooperate with, the operation of national intelligence services (this article has been frequently cited in the West).
>
> **Article 8**: National intelligence services should operate legally, respect and protect human rights, and safeguard the legal interests of individuals and organizations.

While this law does stipulate that any Chinese companies should assist the operation of national intelligence services, it falls short of laying down any specific details for implementation, such as what are the legal interests of companies or what is the legal boundary that China's national intelligence services must respect when requiring Chinese companies to assist their operations. Given that there is no empirical studies of this law in practice, we assume that the controversy around this law may result, in part, from this vagueness. However, not only China, many countries have laws that require their citizens and organizations to cooperate with intelligence services in issues concerning national security. For example, the American Patriot Act (2001) allows the use of National Security Letters (NSLs) by intelligence and law enforcement agencies to seek information from American companies in authorized national security investigations.[57] As the review report on telecoms supply chain from the UK government acknowledges, the Chinese National Intelligence Law is "not the first of its kind"; "Most states have laws that allow for direction for the purposes of national security. Where these arrangements differ across countries is in respect to the rule of law, and the oversight and assurance arrangements for those laws."[58] In other words, China's intelligence law itself may not be that different from Western countries' relevant laws; the West's concerns about this law, and how it works in practice, stem from its distrust of China's authoritarian governing system (as discussed earlier in relation to geopolitical concerns), and the fact that it does not have an independent judiciary branch.

As regards the so-called "backdoor" (referring to malicious functionality intentionally added to hardware or software) accusations linked to Chinese tech companies (especially Huawei), it seems that no solid evidence or a "smoking gun" has been

[57] ACLU (American Civil Liberties Union). *Surveillance under the Patriot Act*. https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act

[58] Department for Digital, Culture, Media & Sport (UK). July 2019. *UK telecoms supply chain review report* (Article 3.16 and footnotes no. 15).

found in Europe, as stated by French Cyber Chief in January 2020.[59] For example, it was reported in 2019 that Vodafone Italy discovered "hidden backdoors" in Huawei equipment that would have allowed the Chinese company to access user data in 2011 and 2012. However, Vodafone clarified that the media report was incorrect: what was found was "nothing more than a failure to remove a diagnostic function [a function common in the industry] after development", and the failure was addressed at the time and it had "no evidence of any unauthorised access [from Huawei]".[60] Similarly, in April 2021, Huawei was reported to have access to the calls of Dutch telecoms operator KPN's 6.5 million mobile users including the Dutch prime minister. Again, KPN said that it had "never observed that Huawei took client information", and none of its suppliers had "unauthorised, uncontrolled or unlimited" access to its networks and systems.[61] Apart from Huawei, a few other Chinese tech firms like DJI (the world's leading commercial drone maker) have also been under heavy scrutiny for espionage concerns from the West. This June, a report from Pentagon admitted that an analysis of two DJI drones built for government use found "no malicious code or intent".[62] However, over a month later, the Pentagon clarified that the report was "unauthorised" and "incorrect".[63]

While "backdoor" concerns over Huawei and other Chinese tech companies are reasonable and understandable, we have not found solid evidence to support them. The UK government, in its 5G supply chain review report, concluded, the risk of Huawei installing "backdoors" in its UK equipment was only "moderate".[64] This conclusion was based on the following reasons: (1) the UK has adopted extensive measures including high-level scrutiny over Chinese companies to mitigate risks like "backdoors"; (2) even if an adversary plans to steal data or perform a cyber-attack, it would not find installing "backdoors" the most effective means to do so, as there exists

[59] Bloomberg (30 January 2020). *No Huawei "smoking gun" in Europe, French Cyber Chief says.* https://www.bloomberg.com/news/articles/2020-01-30/no-huawei-smoking-gun-seen-in-europe-french-cyber-chief-says

[60] BBC News (30 April 2019). *Vodafone denies Huawei Italy security risk*. https://www.bbc.co.uk/news/business-48103430

[61] The Guardian (19 April 2021). *Huawei 'may have eavesdropped on Dutch mobile network's calls.'* https://www.theguardian.com/technology/2021/apr/19/huawei-may-have-eavesdropped-on-dutch-mobile-networks-calls

[62] The Hill (1 June 2021). *Pentagon report clears use of drones made by top Chinese manufacturer*. https://thehill.com/policy/defense/556370-pentagon-report-clears-use-of-drones-made-by-top-chinese-manufacturer?rl=1

[63] The Verge (25 July 2021). The Pentagon says DJI drones still pose a threat, disavowing its own earlier report. https://www.theverge.com/2021/6/1/22463946/dji-drone-ban-pentagon-department-of-interior

[64] Department for Digital, Culture, Media & Sport (UK). July 2019. *UK telecoms supply chain review report,* p.25.

a range of alternative attack routes.[65] We agree with this "backdoor" risk assessment of Huawei (applicable to other Chinese companies) from the UK government. In discussion of potential sabotage risks from Chinese firms using "backdoors" or other methods, some fear that under extreme circumstances such as inter-continental wars, Chinese firms like Huawei might have the ability to "shutdown networks" (the "kill switch" scenario).[66] Given that this perceived sabotage risk is only based on an imaginary account (which we consider highly unlikely), we shall not elaborate further on it.

European countries also have concerns over surveillance technologies from Chinese companies. For example, Serbia's cooperation with Huawei in deploying 1, 000 smart cameras with advanced facial and license plate recognition software in Belgrade, as part of its Safe City project, has raised concerns both within the country and in Europe.[67] Some people worry that China is exporting its authoritarian governing model to other countries through such projects. While such concerns are understandable and reasonable, it should be borne in mind that the risks are not confined to Chinese companies but occur wherever a nation has the capacity to conduct surveillance. Focusing on the surveillance risks posed by one country may distract attention from similar risks from others. According to a report from *Washington Post*, surveillance technology supplied by the U.S. and other Western countries have been used in many countries including authoritarian regimes.[68] Also, the Edward Snowden case revealed that almost all major American tech giants were involved in NSA's espionage and surveillance projects.[69] An alternative course is for each country to ensure surveillance technology not be used for the wrong reason and in wrong places (such as private space). Surveillance technology, complemented by sufficient scrutiny, can be used to improve our safety by preventing and detecting crimes. In the case of Serbia, one concern regarding the Safe City project within the country is that Serbia does not yet have a law on video surveillance. The key to preventing misuses of surveillance technologies is to strengthen regulation.

Content censorship concerns

[65] Ibid.
[66] Tim Rühlig, & Maja Björk (2020). What to make of the Huawei debate? 5G network security and technology dependency in Europe. *Utrikespolitiska Institutet*, 5-6.
[67] Wired (10 August 2021). *Servia's smart city has become a political flashpoint.* https://www.wired.co.uk/article/belgrade-huawei-cameras
[68] The Washington Post (17 January 2019). *How U.S. surveillance technology is propping up authoritarian regimes*. https://www.washingtonpost.com/outlook/2019/01/17/how-us-surveillance-technology-is-propping-up-authoritarian-regimes/
[69] The Guardian (7 June 2013). *NSA Prism program taps into user data of Apple, Google and others.* https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Concerning censorship of content linked to Chinese tech companies, a most recent incident is that, in September 2021, Lithuania accused Chinese firm Xiaomi, the top smartphone vendor in Europe in the second quarter of this year, of having a built-in ability to censor terms such as “Free Tibet” or “democracy movement”.[70] According to a report from Lithuania’s Defence Ministry, although the capability had been turned off for the EU region, but it can be turned on remotely. Xiaomi denied such accusations and announced that it had hired a third-party expert to assess this allegation.[71] It is reported that Germany’s federal cybersecurity watchdog is now conducting a technical examination on Xiaomi phones.[72] Given that this incident is still evolving, we shall not speculate as to the outcome. The general point is that content censorship could become a major security concern for European countries.

The risks of censorship associated with Chinese tech companies are well-illustrated by the TikTok case. In 2019, some media reports revealed that leaked TikTok documents instructed its moderators to suppress content that Beijing deemed politically sensitive such as videos mentioning Tiananmen Square (i.e., 1989 political turmoil in Beijing) and Tibetan independence.[73] TikTok did not deny the existence of this internal moderation guideline, but claimed that the leaked guideline was outdated.[74] To counter censorship (and data security) concerns, the company has adopted a series of measures in recent years: (1) separating Douyin (Chinese version of TikTok) from TikTok, with the latter not available to Chinese domestic users, in order to meet different content rules in domestic and overseas markets; (2) disbanded the whole Beijing team responsible for content moderation in overseas markets in March 2020 and granted the moderation task to local overseas teams; (3) following local laws and cultures in content moderation (in both democratic and authoritarian countries); (4) opening several transparency centres around the globe to illustrate how its content recommendation and moderation is carried out.[75]

---

[70] Reuters (27 September 2021). *China’s Xiaomi hires expert over Lithuania censorship claim.* https://www.reuters.com/technology/chinas-xiaomi-is-engaging-3rd-party-expert-assess-lithuania-censorship-claims-2021-09-27/

[71] Ibid.

[72] Reuters (29 September 2021). *German IT security watchdog examines Xiaomi mobile phone.* https://www.reuters.com/business/media-telecom/german-it-security-watchdog-examines-xiaomi-mobile-phone-2021-09-29/

[73] The Guardian (25 September 2019). Revealed: how TikTok censors videos that do not please Beijing. ttps://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing

[74]Ibid.

[75] Jufang Wang (2020). *From banning to regulating TikTok: Addressing concerns of national security, privacy, and online harms*. Oxford: FLJS Policy Report.

We recently examined the Uighurs-related videos (a topic deemed sensitive by Beijing) on TikTok UK to see how the platform moderates such content and whether censorship can be detected. By searching on TikTok using the keywords “Uighur” and “Uighur Muslims”(Uighurs are an ethnic minority in China and most of them are Muslims), we found that all the popular videos in terms of views are about Xinjiang “genocide”, and that many of which have over 100k views (some near 1 million views). By contrast, pro-China videos, such as those made by several Western vloggers like Daniel Dumbrill and Lee Barrett & Oli Barrett (father and son) who currently live in China, generally only have hundreds or scores of views. In addition, in the comments area of TikTok Uighur-related videos, we frequently read comments complaining that TikTok is supressing pro-China views about the Uighur issue. At the same time, we found comments complaining about pro-China “propaganda” on their TikTok For You Feed. Our initial conclusion is that there is no evidence that ByteDance (owner of TikTok) interfered with content displeasing to Beijing, nor is there evidence that TikTok’s UK team has intentionally censored pro-China content, given that TikTok’s algorithm may distribute content according to UK users’ interests. However, our conclusion still needs to be tested by more systematic research.

Concerns about content censorship are not limited to Chinese tech companies. American tech giants like Facebook and Google have also been criticized for regularly censoring religious and political content at the request of various governments by claiming they simply follow the local laws.[76] Such criticism of censorship practiced by tech companies illustrates the common difficulty of balancing economic profits and respecting freedom of speech. However, from the case study of TikTok, there is reason to conclude that Chinese companies like ByteDance that have ambitions for global expansion are adapting to the overseas media environment and adjusting their moderation practices according to local laws.

4.3 Economic risks

European concerns about Chinese tech companies include economic aspects, such as Chinese investment in Europe’s tech sector and their potential capacity to influence technical standards for critical and emerging technologies like 5G and AI.

Concerns over Chinese investment

[76] The Washington Post (23 February 2021). *Australia shows that Facebook cares about censorship only when it’s profitable*. https://www.washingtonpost.com/outlook/2021/02/23/facebook-australia-pakistan-censorship-blasphemy/
Also see: BBC NEWS (1 December 2020). *Vietnam: Facebook and Google ‘complicit’ in censorship.* https://www.bbc.co.uk/news/world-asia-55140857

Chinese investment in Europe's tech companies saw a rapid increase within a short period before 2019, in response to which Europe took a coordinated approach to strengthen investment screening. For example, from 2016 to 2018, the amount of Chinese venture capital investment in Germany rose from zero to EUR 300 million. Among the investors were Chinese Internet giants Tencent and Alibaba.[77] A notable example was the $5bn acquisition of leading German industrial robot maker Kuka by Chinese electrical appliance firm Midea in 2016.[78] In addition, Chinese companies acquired three semi-conductor manufacturers in Nordic countries in recent years.[79] These events raised a number of concerns in Europe: (1) that strategic acquisitions by Chinese companies would help them to gain cutting-edge technologies; (2) that Europe would lose innovation advantage to China; and (3) that Chinese companies would force their values and governance models on European companies.[80] Against this backdrop, some European countries including Germany, Italy and the UK amended or passed new laws to increase scrutiny over foreign investment in critical technology areas in recent years.[81] At the EU level, the Union introduced an EU-wide framework to coordinate member states in strengthening scrutiny over FDI in 2019 (updated in October 2020), mainly as a response to Chinese investment (as discussed earlier).

European concerns over Chinese investment in the tech sector are justified, especially because a major disadvantage for Europe in global technology competition is that it lacks global tech giants.[82] We support Europe's current digital strategy of achieving digital sovereignty through both "protective mechanisms" (such as stricter screening on foreign investment) and "offensive tools" (state intervention like funding support for tech start-ups at the EU and member states levels) to foster digital innovation.[83] There

[77] Sabrina Korreck (31 March 2021). Exploring the promises and perils of Chinese investment in tech startups: The case of Germany. https://www.orfonline.org/research/exploring-the-promises-and-perils-of-chinese-investments-in-tech-startups-the-case-of-germany/

[78] Techmonitor (21 April 2021). *Is Chinese investment in Europe's technology industry a threat?* https://techmonitor.ai/policy/geopolitics/is-chinese-investment-europe-technology-industry-threat

[79] Ibid.

[80] See for example: Sabrina Korreck (31 March 2021). Exploring the promises and perils of Chinese investment in tech startups: The case of Germany. https://www.orfonline.org/research/exploring-the-promises-and-perils-of-chinese-investments-in-tech-startups-the-case-of-germany/

[81] See for example: The UK government (29 April 2021). *National security bolstered as bill to protect against malicious investment granted royal assent*. https://www.gov.uk/government/news/national-security-bolstered-as-bill-to-protect-against-malicious-investment-granted-royal-assent

[82] Carla Hobbs (ed.). (July 2020). Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry. *European Council on Foreign Relations*.

[83] Tambiama Madiega (2020). *Digital sovereignty for Europe*. EPRS Ideas Paper. European Parliament.

may be a lesson to learn from China in this regard. A protective domestic environment has played a role, not necessarily a decisive role, in the growth of Chinese domestic Internet giants, as a result of keeping American tech giants such as Google and Facebook out of China (Google and most recently LinkedIn chose to retreat from Chinese market due to censorship requirements). Although the main motivation of the Chinese government might be to control public opinion through content censorship, the result is a protected environment for Chinese companies.

However, if Europe is to become a global tech-hub, it is important that an open market will be maintained to attract global investment, talents and tech companies, including those from China. Any measures protective of local companies must be moderate and proportionate. As Sabrina Korreck notes, while posing a range of challenges to Europe, Chinese investment also brings many benefits including promoting the growth of tech start-ups, easier access to Chinese market, a global perspective as well as deep domain expertise and knowledge of the technologies themselves (investors like Tencent and Alibaba have leading technologies in some areas like Fintech).[84] Meanwhile, as mentioned before, from a digital sovereignty perspective, Chinese investment and tech companies in European markets may constitute a much smaller threat when compared to their American peers. In a sense, the entry of Chinese companies and investment can "challenge the quasi monopoly positions of some US tech giants" and stimulate competition.[85] In addition, as some European observers have noted, while the US-China tech rivalry poses problems for Europe, in the sense that it is caught in the middle, it is actually also a great opportunity for Europe. As Saul Klein from the venture capital firm LocalGlobe points out, tensions between the US and China could be a "structural advantage" for Europe, as more companies, in order to be able to trade globally, may choose to put their operations in Europe. This in turn could help bring money, technology and talent to the continent.[86]

Competition around global standards

The increasing potential of Chinese technology companies in influencing technical standards for critical and emerging technologies has caused concerns in the West. For example, in 2018, the Committee on Foreign Investment in the U.S. (CFIUS) noted, in a letter to the American government, that Chinese companies owned a substantial number of 5G patents and had increased their engagement in the international

[84] Sabrina Korreck (31 March 2021). *Exploring the promises and perils of Chinese investment in tech startups: The case of Germany*. https://www.orfonline.org/research/exploring-the-promises-and-perils-of-chinese-investments-in-tech-startups-the-case-of-germany/

[85] Ibid.

[86] Sifted (23 June 2020). *How Europe can dominate the next decade of tech.* https://sifted.eu/articles/european-tech-startups/

standard-setting process. It warned that these developments would lead to a "dominance" of the international 5G standard-setting process by Chinese companies, which, in turn, could adversely affect "national security" of the United States.[87] While the CFIUS has framed the standard-setting of critical technologies as an issue of "national security", technical standards are "primarily an economic rather than security issue".[88] While companies whose technology becomes the industry standard can receive royalty payments from other standards implementors, the patented technologies are available to other companies.

For Europe, which wants to set, rather than follow, global standards in technology areas, it is understandable that Chinese companies' increasing capacity in shaping global standards would be considered as a risk or concern. As stated in the "EU-China—A strategic outlook" document, the rise of China as a "leading technological power" has made it an "economic competitor in the pursuit of technological leadership".[89] Currently, it seems that the US and Europe have strengthened their coordination in the development of global technology standards. The inaugural joint statement of the EU-US TTC, released in September 2021, stated that the council's Working Group on Technology Standards had been tasked to facilitate EU-US coordination and cooperation in technology standards and to defend their "common interest" in international standards activities.[90] While the two sides did not mention China in the statement, they did emphasize that they "support the development of technical standards in line with our core values",[91] indicating that there exists competition around technology standards among countries with different values.

The EU-US coordination and cooperation in technology standards has also been seen in the so-called Open RAN (O-RAN) mechanism, which is an alternative to the current end-to-end 5G technology led by Huawei and two European companies Nokia and Ericsson. The idea of O-RAN technology is to chop up the 5G supply chain into smaller pieces and impose standards on equipment and software firms so their products can work together (a "Lego" approach).[92] As a result, equipment from many smaller

[87] Eli Greenbaum (2018). 5G, standard-setting, and national security. *Harvard Law School National Security Journal*. https://harvardnsj.org/2018/07/5g-standard-setting-and-national-security/

[88] Robert D. Williams (Executive director, Paul Tsai China Center, Yale Law School). (2021). *Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security.* Working paper for the Penn project on the future of U.S.-China Relations.

[89] European Commission. *EU-China-A strategic outlook.* https://ec.europa.eu/info/sites/default/files/communication-eu-china-a-strategic-outlook.pdf

[90] European Commission. *EU-US Trade and Technology Council Inaugural Joint Statement.* https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951

[91] Ibid.

[92] Politico (20 January 2021). After Huawei, Europe's telcos want 'open' 5G networks. https://www.politico.eu/article/oran-reflow-huawei-europe-telecoms-5g/

equipment suppliers can be incorporated into 5G networks, diversifying the current supply chains. Both the US and Europe European countries like the UK and Germany, as well as many telecoms operators, support the O-RAN technology. While the O-RAN Alliance has around 200 members, including major Western tech companies and telecoms operators and also scores of Chinese companies, Huawei, a major 5G patents holder, is excluded from the alliance.[93] In addition, as the U.S. government added, in July 2021, more Chinese tech companies to its export control Entity List, among which was O-RAN Alliance member Kindroid, the survival of this international standard-setting body is now put in doubt. In August 2021, just weeks after the US blacklisted Kindroid, Nokia suspended its participation in the Alliance to avoid US penalties for its having links with Chinese companies that are under sanctions.[94] This shows the development of global technical standards for 5G networks, a mainly economic and technological issue, has been influenced by geopolitical factors.

We consider the EU-US geopolitical approach toward technology standards for critical and emerging technologies not to be an ideal model. As mentioned before, if Chinese companies are excluded from some international standard-setting bodies, it will lead to two separate technical standards systems and create barriers for international trade and cooperation. Before the U.S. started to target Chinese tech companies in 2018, the West had long been an advocate of open and transparent international standard-setting processes. The West had urged China to increase its engagement with international standard-setting institutions, rather than establish its own technical standards to keep foreign companies out of the Chinese market.[95]

5 Policy recommendations

Having identified Europe's digital interests and assessed the risks associated with Chinese tech companies, we now offer a set of policy recommendations for European countries. Our recommendations are guided by European interests in the digital world: digital sovereignty and global technology leadership, which provide a framework within which to work out solutions to risks or at least to find ways of handling risks.

(1) *Prioritising technical solutions over a geopolitical approach in mitigating security risks*

[93] https://www.o-ran.org/membership

[94] O-RAN Alliance. Membership. https://www.lightreading.com/open-ran/nokia-halts-o-ran-work-on-fear-of-us-penalties-for-china-links/d/d-id/771775

[95] Eli Greenbaum (2018). 5G, standard-setting, and national security. Harvard Law School National Security Journal. https://harvardnsj.org/2018/07/5g-standard-setting-and-national-security/

Security risks are inherent with emerging technologies like 5G and AI, as they are by nature dual-use (civilian and military use) and underpin many applications and services such as automatic car driving and Internet of Things.[96] A geopolitical approach is not the most effective way for European countries to mitigate such risks, which are not specific to Chinese tech companies. Vulnerabilities and quality issues can happen to any 5G networks equipment and cyberattacks can be carried out by any threat actors. A geopolitical approach may have two unwanted outcomes for Europe: first, the disruption of global digital supply chains and the fragmentation of global standards on critical and emerging technologies; secondly, the boosting of China's independence in some "bottleneck" technologies (such as advanced microchip production and mobile operating system) from the West in the long run, which would enhance China's position in global technology competition. We therefore propose placing emphasis on technical measures in mitigating Europe's security concerns over Chinese tech companies. As Tim Rühlig and Maja Björk, researchers from The Swedish Institute of International Affairs, argue:[97]

> a ban on Huawei is not an effective solution for generating network security. Other technological measures – first and foremost better encryption, and redundancies coupled with vendor diversity – would be more effective…the idea of banning Huawei stems, rather than from concerns over network security, from a geopolitical logic.

As regards espionage and sabotage risks, possible technical measures include data encryption or requiring Chinese companies to store data of European users within Europe, an approach adopted by an increasing number of countries (such as Russia, China, India, and Brazil). This is also how China settled its security concerns over the American company Apple, which reached an agreement with a Chinese cloud service to store its user data collected in China within the country.[98] Europe may even encourage Chinese companies to join the afore-mentioned GAIA-X platform, a project initiated by Europe "to create a federated and secure data infrastructure".[99] Regarding the security of 5G networks, we agree with the policies of some European countries, the UK for example, in diversifying 5G supply chains to avoid reliance on any single

[96] Robert D. Williams (Executive director, Paul Tsai China Center, Yale Law School). (2021). Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security. Working paper for the Penn project on the future of U.S.-China Relations.

[97] Tim Rühlig, & Maja Björk (2020). What to make of the Huawei debate? 5G network security and technology dependency in Europe. Utrikespolitiska Institutet, 5-6.

[98] Xinhua (27 May 2021). Apple's China data center starts operation. http://www.xinhuanet.com/english/2021-05/27/c_139973639.htm

[99] Gaia-X. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

supplier. However, we deem that excluding Chinese companies from the whole 5G supply chains (as in the case of the UK and some other European countries) may not be necessary, and a more sensible approach would be to impose some restrictions on the role of Chinese companies.

(2) *Strengthening Europe's regulatory power and tackling potential risks through regulatory measures*

We suggest that, in addition to technical solutions, Europe, especially the EU, use its strength in regulating the digital space to reduce risks from foreign tech companies. In August 2021, China passed the *Personal Information Protection Law* (PIPL), which defines the concept and scope of personal information and introduces principles like user consent and minimization of data collection.[100] International observers generally deem that this law is largely modelled on the EU's GDPR.[101] For example, PIPL includes the GDPR-style extraterritorial articles by applying the law to foreign entities dealing with personal information of Chinese residents. It is not known yet whether China's PIPL law will be strictly implemented or whether it will improve the data protection practices of Chinese tech companies. Nevertheless, the passing of the law itself shows that China is learning from the outside world, especially Europe, in terms of digital regulation. China's adoption of the GDPR model is a good example of how Europe can influence China's practices through setting the regulatory example.

We consider AI technologies to be another area where the EU can set the regulatory standards for the world. Currently, the EU is advocating a human-centred and risk-based approach to ensure that AI systems are ethical and trustworthy. This approach differentiates four levels of risk associated with AI technologies in different areas: unaccepted risk (e.g., applications circumventing users' free will), high risk (e.g., critical infrastructure like transport, employment management), limited risk (e.g., chatbots) and minimal risk (e.g., AI-enabled video games), based on which policies regarding AI applications will be made.[102] We regard this risk-based regulatory approach useful for other countries including China in regulating AI technology and applications.

(3) *Making Europe a global high-tech hub and cultivating local tech giants*

[100] Techmonitor (24 August 2021). Here's what 'China's GDPR' means for international businesses. https://techmonitor.ai/policy/heres-what-pipl-china-gdpr-means-for-international-businesses

[101] Ibid.

[102] European Commission. April 2021. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

As a collection of essays on Europe's digital sovereignty points out, while Europe is a regulatory power in digital technologies, it must become "a tech superpower in its own right", as "referees don't win the game".[103] This would require Europe to create a digital environment that is favorable to the growth of local tech firms, while maintaining an open market to attract investment, talents, and technologies from outside. As mentioned earlier, the EU and many European countries, such as the UK, France and Germany, have stated policies and set aside funding to cultivate tech unicorns and future global giants. Excluding Chinese companies and investment does not serve this goal. In fact, the biggest stakeholders of Chinese tech giants Alibaba and Tencent are both foreign companies: Softbank (from Japan) holds 25% stake of Alibaba[104] and the company Naspers (from South Africa) holds 29% share of Tencent.[105] Similarly, almost all major venture capital investors of ByteDance (the owner of TikTok) are from the West.[106] China's example suggests that funding support, no matter its national origin, is crucial for the growth and expansion of tech start-ups (although proper scrutiny and limitations may need to be in place at the same time).

We urge that the US-China tech rivalry be seen as both a challenge and an opportunity for Europe. It is in the interest of Europe to position itself as an alternative global high-tech hub to American Silicon Valley and China's Shenzhen, and as a welcoming destination for tech talents, investment, and companies, regardless of their origins. However, we accept that certain form of "light protectionism", as discussed before, may be necessary to support local tech firms. An open market, complemented by moderate and proportionate protective mechanisms, will be an ideal environment in which to cultivate future tech giants.

(4) *Supporting a multilateral approach to technical standards and leading the development of global standards for emerging technologies*

Global technical standards on 5G (and the future 6G) and other emerging technologies such as AI are crucial for international trade and cooperation over technologies. The West has traditionally supported open and transparent international standard-setting processes. However now it seems that the West is trying to develop standards based on values shared by "like-minded" countries, as evidenced in the inaugural joint statement of the US-EU TTC. While acknowledging the importance of international

[103] Carla Hobbs (ed.). (July 2020). Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry. European Council on Foreign Relations.
[104] Investopedia (26 August 2021). The top 5 Alibaba shareholders.
https://www.investopedia.com/articles/investing/111114/top-five-alibaba-shareholders.asp
[105] Financial Times (7 April 2021). Tencent's biggest investor to trim stake.
https://www.ft.com/content/af7e20b2-00c0-476e-b145-44fbcdd48ee2
[106] Bytedance. https://www.bytedance.com/en/

standard-setting activities, the statement stressed that both parties support the development of technical standards based on their shared values and "wide efforts with like-minded partners".[107] The fact that the Bonn-based O-RAN Alliance, supported by both the US and many European countries, does not include Huawei speaks a lot.

We suggest a different approach, that Europe's long record of supporting multilateralism in international trade be applied to the development of global technical standards for critical and emerging technologies. Fragmented and conflicting global standards are not in the interest of any party. Europe is well-positioned to play an important, even leading, role in the development of global standards by acting as a mediator between the US and China, rather than a follower of the US. While acknowledging its alliance with the US, Europe can better protect its own interests by maintaining independence. Europe as a third party has the potential to establish common ground and to facilitate cooperation on the development of global standards among all parties.

(5) *Promoting European digital values through cooperation and engagement*

Although Europe shares with the US many security concerns over Chinese tech companies, it has in addition its own distinct interests and values in digital areas. For example, Europe has the world's strictest rules in protecting data privacy, while the US does not yet have a data protection law. Europe has also adopted a more cautious and ethical approach towards AI technologies. It is in Europe's interest to uphold and promote its digital values across the world. Europe plainly has genuine concerns about some practices of Chinese tech companies in areas like data privacy, environment protection, and human rights. In our view, it is much more effective to influence China by engaging with it than trying to contain its technology development through exclusion and sanctions. For instance, given that China is a leading actor in AI technologies, it is imperative for Europe to include Chinese companies in the discussion and development of global standards around AI to ensure a future ethically acceptable to all human beings.

[107] European Commission. EU-US Trade and Technology Council Inaugural Joint Statement.
https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951